DEFENSE INFORMATION SYSTEMS AGENCY
JOINT INTEROPERABILITY TEST COMMAND
2001 BRAINARD ROAD
FORT HUACHUCA, ARIZONA 85613-7051

IN REPLY REFER TO: Networks and Transport Division (JTE) 17 June 2004

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the Critical Communications (CritiCom) Integrated Secure Encryption Console (ISEC) 320

References: (a) DOD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01C, "Interoperability and Supportability of Information Technology and National Security Systems," 20 November 2003

1. References (a) and (b) establish the Defense Information Systems Agency, Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification. Additional references are provided in enclosure 1.

2. The Critical Communications (CritiCom) Integrated Secure Encryption Console (ISEC) 320 with no associated software or firmware, hereinafter referred to as the System Under Test (SUT), meets all of the critical interoperability requirements and is certified for joint use in the Defense Switched Network (DSN). The CritiCom ISEC-323, ISEC-Secure Teleconferencing System (STS), and ISEC-STS Deployable were determined by JITC to be functionally identical to the SUT for interoperability certification purposes, and are also certified for joint use in the DSN. The SUT was tested primarily to determine that it appeared transparent when connected between the video teleconferencing (VTC) equipment and the inverse multiplexer and had no adverse effect on 384 kbps bandwidth on demand in interoperability group mode 1 VTC calls. JITC tested the SUT as set forth in reference (c) using test procedures derived from reference (d). This certification expires upon changes that affect interoperability, but no later than three years from the date of this memorandum.

3. This certification is based on interoperability testing conducted by the JITC from 3 through 6 February 2004 at the Global Information Grid Network Test Facility, Fort Huachuca, AZ, in an operationally realistic environment that is similar to that of the DSN. The Certification Testing Summary (enclosure 2) documents the test results and describes the test network. Users should verify interoperability before deploying the SUT in an environment that varies significantly from that described.

4. The certification of the SUT is based upon evaluation of the platforms using the Capability Requirements (CRs) derived from reference (c). The CRs used to evaluate the interoperability of the application are listed in table 1. Table 2 lists the components of the SUT.

Table 1. SUT Interface Interoperability Status

Platform	Interface	Critical	Status	Capability Requirement Met
ISEC 320 ISEC 323 ISEC STS	Serial EIA-366	Yes	Certified	BONDING Mode 1 VTC
	Serial EIA-449[1]	No	Certified	
	Serial EIA-530[1]	No	Certified	

Legend:
BONDING - Bandwidth ON Demand INteroperability Group
EIA - Electronics Industries Alliance
ISEC - Integrated Secure Encryption Console
STS - Secure Teleconferencing Equipment
SUT - System Under Test
VTC - Video Teleconferencing

Note: Only one of either serial interface required (EIA 449 or EIA 530).

Table 2. SUT Components

Board Name	Description
CC-VWS	Modality Switch
CC-VWS-IP	H.323 Modality Switch
CC-DI-366	Dial Isolator
CC-CM-200	Power Module
CC-3014-2	KIV-7 Housing
CC-5020-CL	KIV-19 Housing
CC-Mode	Power Module

Legend:
CC - CritiCom
CL - Control Leads
CM - Control Module
DI - Dial Isolator
H.323 - Codec protocol for IP
IP - Internet Protoocol
KIV - Not an acronym
SUT - System Under Test
VWS - Not an acronym

5. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil/. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet), or http://199.208.204.125/ (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi.

6. The JITC point of contact is Mr. John Hooper, DSN 879-5041, commercial (520) 538-5041, FAX DSN 879-4347, or e-mail to hooperj@fhu.disa.mil.

FOR THE COMMANDER:

2 Enclosures a/s

LESLIE CLAUDIO
Chief
Networks and Transport Division

Distribution:
Joint Staff J6I, Room-1E565, Pentagon, Washington, DC 20318-6000
Joint Interoperability Test Command, Washington Operations Division, NSWC, ATTN: JT1, Building 900, 101 Strauss Avenue, Indian Head, MD 20640-5035
Defense Information Systems Agency, GIG Enterprise Services Engineering Directorate, NETCENTRICITY, REQUIREMENTS, ANALYSIS & ASSESSMENTS BRANCH, ATTN: GE333, Rm. 244, 5600 Columbia Pike, Falls Church, VA 22041-2770
Defense Information Systems Agency, GIG-Combat Support Directorate, DSN SYSTEMS MANAGEMENT BRANCH, ATTN: GS235, Rm. 5W248A, 5275 Leesburg Pike, Falls Church, VA 22041
Office of Chief of Naval Operations (N61C22), CNON6/7, 2000 Navy Pentagon, Washington, DC 20350
Headquarters US Air Force, AF/XICC, 1250 Pentagon, Washington, DC 20330-1250
Department of the Army, Office of the Secretary of the Army, G-6/ASA (ALT), ATTN: ASAALT (SAAL-SSI), 103 Army Pentagon, Washington, DC 20310-0103
US Marine Corp (C4ISR), MARCORSYSCOM, 2200 Lester Street, Quantico, VA 22134
DOT&E, Strategic and C3I Systems, 1700 Defense Pentagon, Washington, DC 20301-1700
US Coast Guard, COMDT/G-SCE (C4), 2100 2nd Street SW, Washington, DC 20593
Office of Assistant Secretary of Defense, OASD(NII)/DoD CIO, Crystal Mall 3, 7th Floor, Suite 700, 1931 Jefferson-Davis Hwy, Arlington, VA 22202
Office of Under Secretary of Defense, OUSD(AT&L), Room 3E144, 3070 Defense Pentagon, Washington, DC 20301
US Joint Forces Command, J6I, C4 Plans and Policy, 1562 Mitscher Ave, Norfolk, VA 23551-2488
Defense Intelligence Agency, ATTN: DS-CIO, Bldg 6000, Bolling AFB, Washington, DC 20340-3342
National Security Agency, ATTN: DT, Suite 6496, 9800 Savage Road, Fort Meade, MD 20755-6496
Commander, Defense Information Systems Agency (DISA), ATTN: GS23 (Mr. Osman), Room 5w23, 5275 Leesburg Pike (RTE 7), Falls Church, VA 22041

ADDITIONAL REFERENCES

(c) Defense Information Systems Agency (DISA), Defense Switched Network (DSN) Generic Switching Center Requirements (GSCR)," 8 September 2003
(d) Draft Joint Interoperability Test Command, "Defense Switched Network Generic Switch Test Plan (GSTP)" 17 June 1999

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Critical Communications (CritiCom) Integrated Secure Encryption Console (ISEC)-320, hereinafter referred to as the system under test (SUT) (no associated software or firmware).

2. PROPONENT. Defense Information Systems Agency (DISA).

3. PROGRAM MANAGERS. Mr. Howard Osman, GS23, Room 5W23, 5275 Leesburg Pike, Falls Church, VA, 22041, e-mail: Osmanh@ncr.disa.mil.

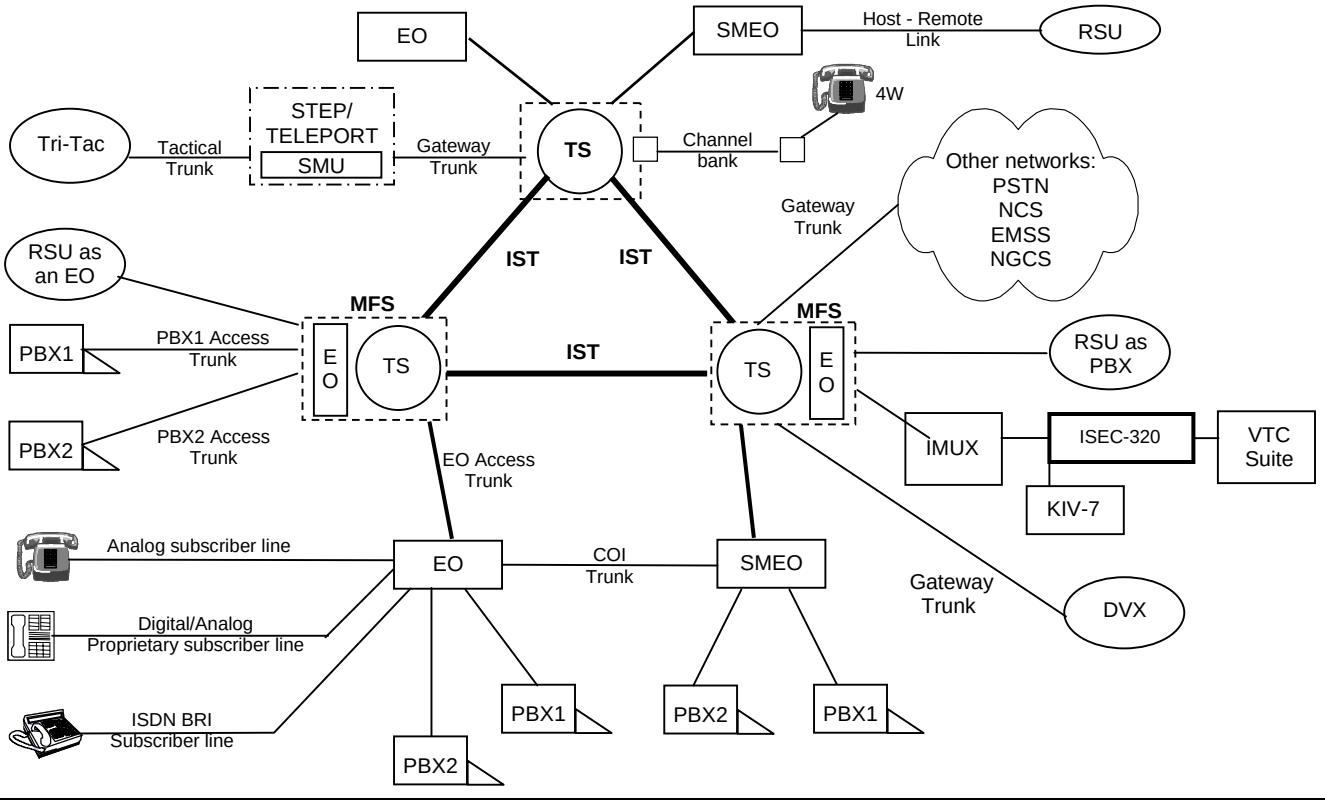
4. TESTERS. Joint Interoperability Test Command (JITC), Ft. Huachuca, AZ.

5. SYSTEM UNDER TEST DESCRIPTION. The SUT is a secure/non-secure modality switch that integrates with standard video teleconferencing (VTC) console industry codecs, encryption, and networking products to produce Type 1 Secure/Non-Secure dual-use videoconferencing systems solutions. Marketed as ISEC products, this family of solutions is sold in a variety of forms to allow clients to conduct secure and non-secure VTC sessions in both fixed and deployable scenarios using ISDN and/or IP connectivity (H.320 and H.323). The CritiCom ISEC-323, ISEC-Secure Teleconferencing System (STS), and ISEC-STS Deployable were determined by JITC to be functionally identical to the SUT for interoperability certification purposes, and are also certified for joint use in the DSN.

6. OPERATIONAL ARCHITECTURE. The Generic Switching Center Requirements (GSCR) Defense Switched Network (DSN) operational architecture is depicted in figure 2-1.

7. REQUIRED SYSTEM INTERFACES. The Capability Requirements (CRs) used to evaluate the interoperability of the application are listed in table 2-1. Interoperability certification of the interfaces is based on meeting criteria from the CRs. The SUT components are listed in table 2-2.

8. TEST NETWORK DESCRIPTION. The SUT was tested at JITC's Network Engineering and Integration Laboratory in a manner and configuration similar to that of the test network configuration in figure 2-2.



Legend:

4W	- 4 wire
BRI	- Basic Rate Interface
COI	- Community of Interest
DSN	- Defense Switched Network
DVX	- Deployable Voice Exchange
EMSS	- Enhanced Mobile Satellite System
EO	- End Office
IMUX	- Inverse Multiplexer
ISDN	- Integrated Services Digital Network
ISEC	- Integrated Secure Encryption Console
IST	- Interswitch Trunk
MFS	- Multifunction Switch
MLPP	- Multi-Level Precedence and Preemption
NATO	- North Atlantic Treaty Organization
NCS	- National Communications System
NGCS	- NATO Gateway Communications Switch
PBX1	- Private Branch Exchange 1 (MLPP)
PBX2	- Private Branch Exchange 2 (non-MLPP)
PSTN	- Public Switched Telephone Network
RSU	- Remote Switching Unit
SMEO	- Small End Office
SMU	- Switched Multiplexer Unit
STEP	- Standardized Tactical Entry Point
Tri-Tac	- Tri-Service Tactical
TS	- Tandem Switch
VTC	- Video Teleconferencing

Figure 2-1. DSN Architecture

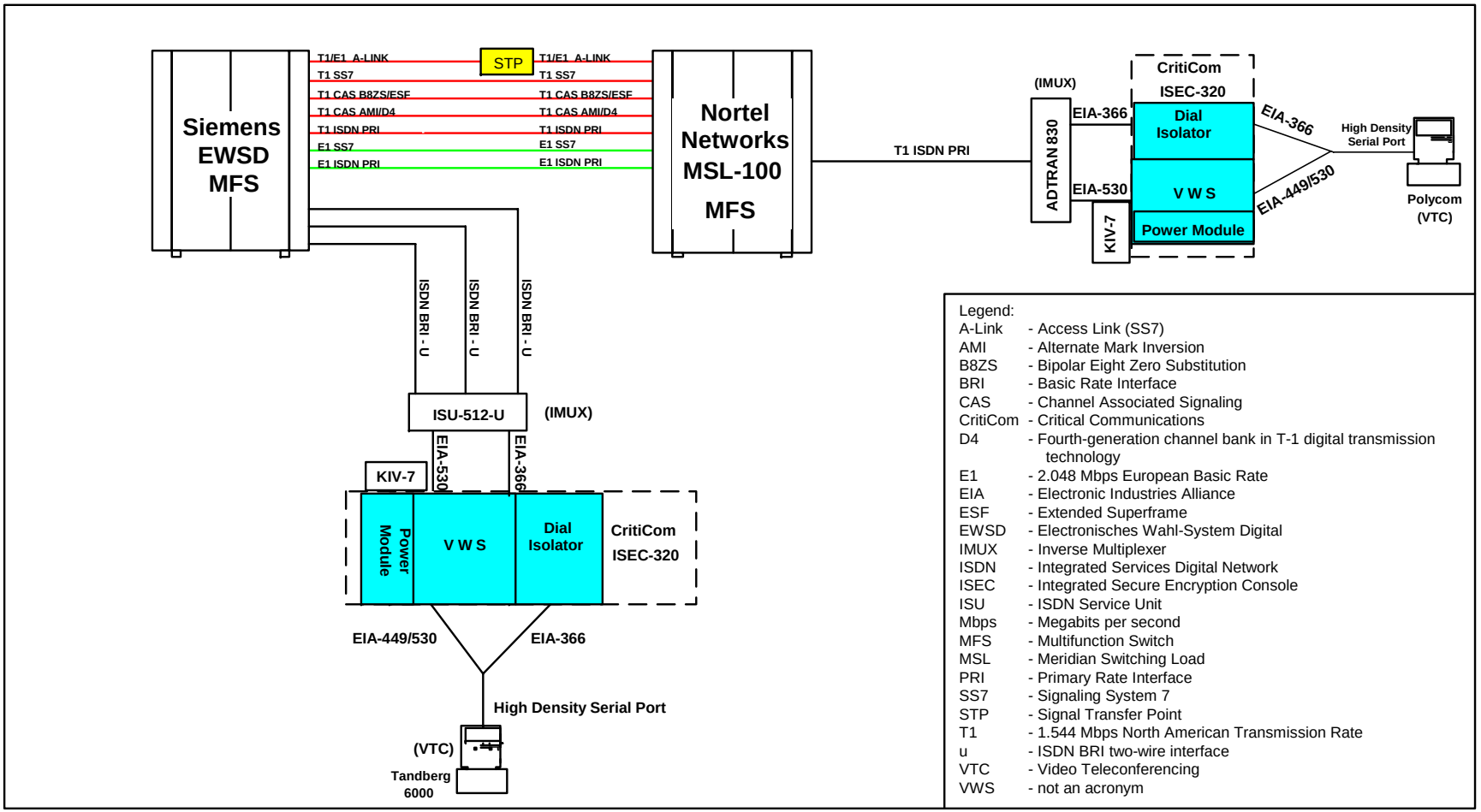


Figure 2-2. Test Network Configuration

Table 2-1. SUT Interface Interoperability Status

Platform	Interface	Critical	Status	Capability Requirement Met
ISEC 320 ISEC 323 ISEC STS	Serial EIA-366	Yes	Certified	BONDING Mode 1 VTC
	Serial EIA-449[1]	No	Certified	
	Serial EIA-530[1]	No	Certified	

Legend:
BONDING - Bandwidth ON Demand INteroperability Group
EIA - Electronics Industries Alliance
ISEC - Integrated Secure Encryption Console
STS - Secure Teleconferencing Equipment
SUT - System Under Test
VTC - Video Teleconferencing

Note: Only one of either serial interface required (EIA 449 or EIA 530).

9. SYSTEM CONFIGURATIONS. Table 2-2 lists the hardware components used by the SUT.

Table 2-2. SUT Components

Board Name	Description
CC-VWS	Modality Switch
CC-VWS-IP	H.323 Modality Switch
CC-DI-366	Dial Isolator
CC-CM-200	Power Module
CC-3014-2	KIV-7 Housing
CC-5020-CL	KIV-19 Housing
CC-Mode	Power Module

Legend:
CC - CritiCom
CL - Control Leads
CM - Control Module
DI - Dial Isolator
H.323 - Codec protocol for IP
IP - Internet Protocol
SUT - System Under Test
VWS - Not an acronym

10. TEST LIMITATIONS. None.

11. TEST RESULTS.

a. Discussion. The SUT uses its modality switch to smoothly transition from a non-secure 384-kilobits per second (kbps) bonded VTC call (modality switch power-on) to a secure 384-kbps bonded VTC (modality switch power-off) call. The VTC call attempts were made using both Basic Rate Interfaces (BRI) and Primary Rate Interfaces (PRI) connected to an Integrated Access Switch or an inverse multiplexer (BRI only) which in turn were serially connected to the SUT. The SUT isolates the dialing stream from the data stream by using an EIA-366 interface dial isolator module along with either an EIA-449 or EIA-530 interface to pass the data stream. The modality switch allows the user to seamlessly transition from one call type to another with the flip of a switch. Testing included call strings

utilizing KIV-7 encryption devices and call strings without encryption devices. The SUT handled each type of call attempt flawlessly.

b. Summary. The SUT is certified for joint use in the DSN in accordance with the requirements set forth in reference (c). When connected to the interfaces certified in this letter, the SUT was transparent to the switching systems or lines interfaced, causing no degradation of service or negative impact, and met all the critical interoperability requirements.

12. TEST AND ANALYSIS REPORT. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil/. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet), or http://199.208.204.125/ (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi.